UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/761,512	01/20/2004	Philippe Leyendecker	PF030028	2983

7590 11/16/2006

JOSEPH S. TRIPOLI
THOMSON LICENSING INC.
SUITE 200
2 INDEPENDENCE WAY
PRINCETON, NJ 08540

EXAMINER	
PARRA, OMAR S	

ART UNIT	PAPER NUMBER
2621	

DATE MAILED: 11/16/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/761,512	LEYENDECKER ET AL.	
	Examiner	Art Unit	
	Omar Parra	2621	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *20 January 2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-14* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-14* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *01/20/2004*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Priority

1. Acknowledgment is made of applicant's claim for foreign priority based on application 03/00941 filed in France on January 20, 2003, and European application 03291099.4 filed on May 7, 2003.

Information Disclosure Statement

2. The information disclosure statement filed on 01/20/2004 was acknowledged by Examiner for prosecution purposes.

Specification

3. Preliminary amendments to the Specification submitted on 01/20/2004 were acknowledged by Examiner for prosecution purposes.

Claim Objections

4. **Claims 1, 2, 4-6, 11 and 14** are objected to because of the following informalities Appropriate correction is required.

5. Consider **Claim 1:** Third indentation creates confusion. As understood by the examiner, indentation in this claim introduces a new component of the system mentioned at line 4. In line 8, no new element of said system is introduced but indentation is used to give characteristics of something, which is not clearly stated. However, examiner construes those characteristics to be functional specifications of the system.

6. Consider **Claim 2**: Referred element was not previously mentioned. On line 15, "the" should be replaced by "a" since no data broadcasting system was mentioned in claim 1.

7. Consider **Claim 4**: An extra character is unnecessarily shown. At the first line of the claim, the number "4" standing in between words "to" and "Claim" should be removed, as understood by examiner to have no meaning.

8. Consider **Claims 4 and 6**: Having two logical operators adjacent to each other. On lines 22 and 33 of respective claims 4 and 6, "and/or" is shown to give the alternative of treating the terms "descrambling" and "deciphering" as different or similar to each other, respectively. However, as construed by examiner and as stated by applicant in page 1 lines 19-22, these two terms represent the same process. This makes the use of the "and" improper and the "or" redundant. For purposes of examination, the "or" is considered to have the alternative to choose between two equivalent terms. The same interpretation is made when "descrambling/deciphering" is used in lines 23 and 34, of claims 4 and 6, respectively.

9. Consider **Claim 5**: Extra word is used. On line 29, the word "and" should be removed and a pair of commas should be added. One comma should be placed between "data" and "which" at line 28, while the other one after "digital terminal" at line 29. In this way, everything after said "and" would clearly refer to the "protected data" as construed by the examiner. Appropriate correction is required.

10. Consider **Claim 11**: Incorrect word is used. As construed by the examiner, the word "ends" at the fourth line of the claim, should be replaced with "sends".

11. Consider **Claim 14**: Incorrect word is used. As construed by the examiner, the word "to" at line 10 should be replaced with "the".

Claim Rejections - 35 USC § 102

12. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

13. Claims **1 ,8,9 and 13** are rejected under 35 U.S.C. 102(e) as being anticipated by Weber (Publication No. US 2004/0098583 A1).

14. Consider **claim 1**, Weber teaches a system (Fig.1) for receiving broadcast digital data comprising:

a master digital terminal ("Sending device", Fig.1 - although a 'master' device is able to send or receive), and

at least one slave digital terminal ("Receiving device", Fig. 1- although a 'slave' device is able to send or receive) connected to the master terminal by a link ("Communication channel", Fig. 1) and able to receive ("...that the receiver is authorized to receive the digital content", [0003] line 9-10) protected digital data (Since the invention solves problems of "DTCP, PGP, Kerberos, HDCP", [0003] lines 11-13, systems, it is inherent that transmitted data is encrypted)

characterized in that said slave digital terminal can access said protected data only if information necessary for accessing said data ("...shared secrets and key exchange..." [0003], lines 8-9), and received by the master ("Sending device", Fig.1) digital terminal is sent by way of said link ("Communication channel", Fig. 1) to the slave digital terminal ("Receiving device", Fig. 1) within a predetermined deadline ("...predetermined response time limit.", [0016] line 9).

15. Consider **claim 8**, and as applied on claim 1, Weber teaches a system in which the predetermined deadline ("...predetermined response time limit." [0016] line 9) is counted down from the dispatching ("T1", Fig.1) by the slave (Being 'master' or 'slave' is a functional difference and no structural) digital terminal ("Sending device", Fig. 1) of a message ("Acknowledgment Request", Fig. 1) to the master (Being 'master' or 'slave' is a functional difference and no structural) digital terminal ("Receiving device", Fig.1).

16. Consider **claim 9,** and as applied on claim 1, Weber teaches that his invention is also applicable in a broadcasting system scheme ("In other embodiment ... a sending device 50 may send digital content to receiving devices in more than one geographical area...", Fig.3), in which the predetermined deadline is counted down ("Response time", Fig.1) from the dispatching ("T1", Fig.1), by the broadcasting system of the data ("Sending device 50", Fig.3), of a message to the master digital terminal (71, Fig. 3).

17. Consider **claim 13**, Weber teaches a digital terminal ("Receiving device", Fig. 1- although a 'slave' device is able send or receive) intended to receive ("...that the

receiver is authorized to receive the digital content", [0003] line 9-10) protected digital data (Since the invention solves problems of "DTCP, PGP, Kerberos, HDCP", [0003] lines 11-13, systems, it is inherent that transmitted data is encrypted), wherein the digital terminal can access said protected data only if information necessary for accessing said data ("...shared secrets and key exchange...", [0003] lines 8-9) and received by another digital terminal to which it can be connected ("Sending device", Fig.1 - although a 'master' device is able to send or receive), is sent to it by this other terminal ("Sending device", Fig.1 - although a 'master' device is able to send or receive) within a predetermined deadline ("...predetermined response time limit.", [0016] line 9).

18. **Claim 14** is rejected under 35 U.S.C. 102(b) as being anticipated by Benardeau et al. (Patent No. US 6,904,522 B1).

19. Consider **claim 14**, Benardeau et al. teaches a first digital terminal (50, Fig.4) intended to be connected to a second digital terminal (12, Fig.4), wherein said first digital terminal is able to receive information necessary for said second terminal to access to protected digital data (ECMs containing the Control Words CW to descramble the signal, col. 11, lines 63-65) and is able to dispatch said information to said second terminal (83, Fig.6).

Claim Rejections - 35 USC § 103

20. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the

invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

21. Claims **2-7 and 10** are rejected under 35 U.S.C. 103(a) as being unpatentable over Weber (Publication No. US 2004/0098583 A1) in view of Benardeau et al. (Patent No. US 6,904,522 B1).

22. Consider **claim 2**, and as applied on claim 1, Weber teaches all the limitations of the system of claim 1, as discussed before, and further teaches that his invention is also applicable in a broadcasting system scheme ("In other embodiment ... a sending device 50 may send digital content to receiving devices in more than one geographical area..." Fig.3). On the other hand, Weber fails to explicitly teach that the information necessary for accessing the protected data, which is received by the master digital terminal, originates from the data broadcasting system. However, Benardeau et al. does disclose having a master digital terminal (43, Fig.3) whose information necessary for the slave to access protected data ("monthly exploitation key, Kex" col. 13, line 16 or "Kex" Fig. 3, with which master will descramble the CW needed for the slave to descramble data or "Alternatively, the ECM messages...may be received directly by the master decoder...", col. 14 lines 56-59) is originated at the broadcasting system (41, Fig. 3 or see column 11 lines 48-53).

23. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to have broadcasted the "Kex" mentioned above from the broadcasting system ("Sending device 50", Fig. 3) to the master receiver (71, Fig.3) for the benefit of remotely and periodically update that same "Kex" without sending someone to physically do it. In addition, it is important to point out that Bernardeau's

invention serves as an example of how "a traditional digital rights management system", as per Weber [0003] lines 7-9, works.

24. Consider **claim 3**, and as applied on claim 2, Benardeau further teaches a system wherein said information for accessing the data (75, Fig. 6, which includes the CW for the slave to descramble data) received by the master digital terminal (30, Fig.6) is transformed (80 and 82, Fig. 6) before being sent (83, Fig.6) to the slave digital terminal (52, Fig.6).

25. Consider **claim 4**, and as applied on claim 3, Benardeau teaches a system in which the transformation comprises a descrambling and/or deciphering of said information in the master digital terminal (" ...control word is decrypted at 80..." col.15 line 1), the descrambling/deciphering being performed with the aid of keys received beforehand (81, Fig. 6) by the master digital terminal of the broadcasting system.

26. Consider **claim 5**, and as applied on claim 1, Benardeau teaches a system according to Claim 1, wherein the information necessary for accessing the protected data (75, Fig. 6, which includes the CW for the slave to descramble data) which is received by the master digital terminal originates from the slave digital terminal (75, Fig.6) and is transformed before being resent to the slave digital terminal (80 and 82, Fig. 6).

27. Consider **claim 6,** and as applied on claim 5, Benardeau teaches a system in which the transformation comprises a, descrambling and/or deciphering (" ...control word is decrypted at 80..." col.15 line 1) of said information in the master digital terminal **(30, Fig.6)**, the descrambling/deciphering being performed with the aid of keys received beforehand by the master digital terminal of the broadcasting system (81, Fig. 6).

28. Consider **claim 7**, and as applied on claim 1, Benardeau teaches a system in which the protected digital data comprise television services ("N data stream", Fig.3, which represents TV programs when referring to TV broadcasting, see col.9, lines 40-46) scrambled by keys ("Control Words") and in which the information necessary for accessing said data belongs to the set comprising:

a message containing access entitlements ("Unique" EMMs addressed to the unique identifier of the smartcard", col.10 lines 5-6... "...to control access to rights associated with the programs transmitted", col.10 lines 8-9) to the services for the slave digital terminal (Since the slave also possesses a unique smartcard, EMMs are able to be uniquely routed to it and have info related to its access rights);

a message (The EMM monthly update), containing parameters for extracting (81, Fig. 6) from the data stream received by the slave digital terminal ("N", Fig. 3) a message containing access entitlements to the services for the slave digital terminal (ECM inside N, Fig. 3 or see col. 14 lines 51-59) ;

a message (62, Fig.5) containing partial (One of two keys needed for master-slave communication) information ("KpubT" or 68, Fig. 5) enabling the slave

digital terminal to reconstruct its access entitlement (Without this partial information, no information can be transferred between the two) to the services ;

a message (71, Fig.5) containing keys ("KpubT" and "Ks", Fig 5) for descrambling said protected digital data (Without the combination of those keys no master-slave communication can be achieved, and consequently, no data can be descrambled).

29. Consider **claim 10,** and as applied on claim 1, Benardeau teaches a system in which the information necessary for accessing the protected data ("...the ECM containing the Control Word CW to descramble the signal", col. 11 lines 63-65), is sent from the master digital (30, Fig.6) terminal to the slave digital terminal **(52, Fig.6)** while being protected by enciphering (82, Fig.6) using a key shared by the two terminals (83 and 84, Fig.6, "Ks, Symmetrical Key").

30. Claim **11** is rejected under 35 U.S.C. 103(a) as being unpatentable over Weber (Publication No. US 2004/0098583 A1) in view of Benardeau et al. (Patent No. US 6,904,522 B1).

31. Consider **claim 11**, and as applied on claim 1, Weber teaches all the limitations of claim 1 as rejected above, and further teaches that his invention is also applicable in a broadcasting scheme having a broadcasting system ("Sending device 50", Fig.3), a master digital terminal ("Receiving device 71", Fig. 3) and a slave digital terminal ("Receiving device 72", Fig.3), in which the master digital terminal ("Receiving device

71", Fig. 3) sends information necessary for accessing the data ("...shared secrets and key exchange...", [0003] lines 8-9) to the slave terminal ("Receiving device 72", Fig.3) only if it receives a response from the slave terminal within a second predetermined deadline counting from the receipt of the response by the master terminal (Having a slave device, adds up another "receiving device" to the right of Fig.1 creating the broadcasting system shown in Fig. 3. Consequently, another "predetermined response time" between the two "receiving devices" will be created and being able to measure it from either one since they are structurally the same). On the other hand, although Weber teaches using "digital authentication such as shared secrets and key exchange" ([0003] lines 8-9), he fails to explicitly teach how they are exchanged and where those secrets are coming from.

32. However, Benardeau et al. teaches having a broadcasting system (41, Fig.3 or Fig.2 except blocks 8-13 and 30) from where all data, information necessary to access said data ("...the ECM containing the Control Word CW to descramble the signal", col. 11 lines 63-65) and keys for device communication ("EMM's") are sent. In addition, Benardeau teaches how those keys are exchanged between devices. In Fig.5, two broadcasted EMMs (62, Fig. 5) containing a pair of keys ("KpriT", 64 and "KpubT"68), which are stored at the master digital terminal (30, Fig.5) and the slave digital terminal (52, Fig.5). Having "KpubT", the slave can encrypt ("fa" ,70 Fig.5) any message it sends to the master (30, Fig.5), including a random slave-generated "secret code" (69, Fig.5), which will be sent and stored at the master with the aid of "KpriT". The master terminal

will only be able to understand messages from other devices, only if they are encrypted with "KpubT".

33. Therefore, it would have been obvious to an ordinary skilled in the art at the time of the invention to provide the broadcasted secret code (pair of keys ("KpriT" and "KpubT") from the broadcasting system, as taught by Benardeau, to Weber's digital authentication, for the benefit of having a more secure inter-device communication.

34. Consider claim **12,** and as applied to claim 11, the combined teachings of Weber and Benardeau et al. teach having a system in which the secret code ("KpriT and KpubT", Fig.5) is received by the master digital terminal (30, Fig.5) and the slave digital terminal (52, Fig.5). On the other hand, the combination fails to explicitly teach that said secret code to be scrambled with the aid of keys sent beforehand to said terminals by the data broadcasting system.

35. However, the combination of Weber and Benardeau teaches the broadcasting system can transmit more than one set of keys to the master and slave terminals ("In a further realization a second layer of authorization may be provided...a certificate Ct(KpubMan) comprising the key KpubMan encrypted by KpriSystem...", which can be a plain private key plus the certificate as done for KpriT before, "...is stored in the card 30", col.14 lines 36-40 and then "the certificate is sent to 52 which decrypts it", col. 14 lines 41-45).

36. Therefore, it would have been obvious to an ordinary skilled in the art at time of the invention to have sent another set of public/private keys to both master and slave

terminals after "Kprit" and "Kpubt" were sent, and in the same way they were exchanged as described in claim 11 to replace the randomly generated key "Ks" for the benefit of having more security since it is not enough to simply pass an encrypted version of R (random value) since a random value could be substituted for a different random sequence of bits by the attacker.

Double Patenting

37. A rejection based on double patenting of the "same invention" type finds its support in the language of 35 U.S.C. 101 which states that "whoever invents or discovers any new and useful process ... may obtain a patent therefor ..." (Emphasis added). Thus, the term "same invention," in this context, means an invention drawn to identical subject matter. See *Miller v. Eagle Mfg. Co.*, 151 U.S. 186 (1894); *In re Ockert*, 245 F.2d 467, 114 USPQ 330 (CCPA 1957); and *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970).

A statutory type (35 U.S.C. 101) double patenting rejection can be overcome by canceling or amending the conflicting claims so they are no longer coextensive in scope. The filing of a terminal disclaimer cannot overcome a double patenting rejection based upon 35 U.S.C. 101.

38. Claims **1-14** provisionally rejected under 35 U.S.C. 101 as claiming the same invention as that of claims **1-14** of copending Application No. 10/766,092. This is a provisional double patenting rejection since the conflicting claims have not in fact been patented.

39. Claims **1-14** directed to the same invention as that of claims **1-14** of commonly assigned Application No. 10/766,092. The issue of priority under 35 U.S.C. 102(g) and possibly 35 U.S.C. 102(f) of this single invention must be resolved.

Since the U.S. Patent and Trademark Office normally will not institute an interference between applications or a patent and an application of common ownership (see MPEP Chapter 2300), the assignee is required to state which entity is the prior inventor of the conflicting subject matter. A terminal disclaimer has no effect in this situation since the basis for refusing more than one patent is priority of invention under 35 U.S.C. 102(f) or (g) and not an extension of monopoly.

Failure to comply with this requirement will result in a holding of abandonment of this application.

40. A comparison of the claims of both applications follows:

Leyendecker et al., 10/761,512	**Louzir et al., 10/766,092**
1. System for receiving broadcast digital data comprising: a master digital terminal, and at least one slave digital terminal connected to the master by a link and able to receive protected digital data characterized in that said slave digital terminal can access said protected data only if information necessary for accessing said data, and received by the master digital terminal is sent by way of said link to the slave digital terminal within a predetermined deadline.	1. System for receiving broadcast digital data comprising : a master digital terminal, and at least one slave digital terminal connected to the master terminal by a link and able to receive protected digital data, characterized in that said slave digital terminal can access said protected data only if information necessary for accessing said data and received by the master digital terminal is sent by way of said link to the slave digital terminal within a predetermined deadline.
2. System according to Claim 1, wherein the information necessary for accessing the protected data which is received by the master digital terminal originates from the data broadcasting system.	2. System according to Claim 1, wherein the information necessary for accessing the protected data which is received by the master digital terminal originates from the data broadcasting system.

3. System according to Claim 2, wherein said information for accessing the data received by the master digital terminal is transformed before being sent to the slave digital terminal.	3. System according to Claim 2, wherein said information for accessing the data received by the master digital terminal is transformed before being sent to the slave digital terminal.
4. System according to **4** Claim 3, in which the transformation comprises a descrambling and/or deciphering of said information in the master digital terminal, the descrambling/deciphering being performed with the aid of keys received beforehand by the master digital terminal of the broadcasting system.	4. System according to Claim 3, in which the transformation comprises a descrambling and/or deciphering of said information in the master digital terminal, the descrambling/deciphering being performed with the aid of keys received beforehand by the master digital terminal of the broadcasting system.
5. System according to Claim 1, wherein the information necessary for accessing the protected data which is received by the master digital terminal originates from the slave digital terminal and is transformed before being resent to the slave digital terminal.	5. System according to Claim 1, wherein the information necessary for accessing the protected data which is received by the master digital terminal originates from the slave digital terminal and is transformed before being resent to the slave digital terminal
6.System according to Claim 5, in which the transformation comprises a, descrambling and/or deciphering of said information in the master digital terminal, the descrambling/deciphering being performed with the aid of keys received beforehand by the master digital terminal of the broadcasting system.	6. System according to Claim 5, in which the transformation comprises a descrambling and/or deciphering of said information in the master digital terminal, the descrambling/deciphering being performed with the aid of keys received beforehand by the master digital terminal of the broadcasting system.
7. System according to Claim 1, in which the protected digital data comprise television services scrambled by keys and in which the information necessary for accessing said data belongs to the set comprising: a message containing access entitlements to the services for the slave digital terminal; a message containing	7. System according to Claim1, in which the protected digital data comprise television services scrambled by keys and in which the information necessary for accessing said data belongs to the set comprising : - a message containing access entitlements to the services for the slave digital terminal ; - a message containing

parameters for extracting from the data stream received by the slave digital terminal a message containing access entitlements to the services for the slave digital terminal ; a message containing partial information enabling the slave digital terminal to reconstruct its access entitlement to the services ; a message containing keys for descrambling said protected digital data.	parameters for extracting from the data stream received by the slave digital terminal a message containing access entitlements to the services for the slave digital terminal ; - a message containing partial information enabling the slave digital terminal to reconstruct its access entitlement to the services ; - a message containing keys for descrambling said protected digital data
8. System according to Claim 1, in which the predetermined deadline is counted down from the dispatching by the slave digital terminal of a message to the master digital terminal.	8. System according to Claim1, in which the predetermined deadline is counted down from the dispatching by the slave digital terminal of a message to the master digital terminal.
9. System according to Claim 1, in which the predetermined deadline is counted down from the dispatching by the broadcasting system of the data of a message to the master digital terminal.	9. System according to Claim 1, in which the predetermined deadline is counted down from the dispatching by the broadcasting system of the data of a message to the master digital terminal.
10. System according to Claim 1, in which the information necessary for accessing the protected data, is sent from the master digital terminal to the slave digital terminal while being protected by enciphering using a key shared by the two terminals.	10. System according to Claim 1, in which the information necessary for accessing the protected data is sent from the master digital terminal to the slave digital terminal while being protected by enciphering using a key shared by the two terminals.
11.System according to Claim 1, in which the master digital terminal and slave digital terminal furthermore receive from the data broadcasting system a secret code and in which the master digital terminal ends said information necessary for accessing the data to the slave terminal only if it receives said secret code from the slave terminal within a second predetermined deadline counting from the receipt of the secret code by the master terminal.	11. System according to Claim 1, in which the master digital terminal and slave digital terminal furthermore receive from the data broadcasting system a secret code and in which the master digital terminal ends said information necessary for accessing the data to the slave terminal only if it receives said secret code from the slave terminal within a second predetermined deadline counting from the receipt of the secret code by the master terminal.

12. System according to Claim 11, in which the secret code received by the master digital terminal and by the slave digital terminal is scrambled with the aid of keys sent beforehand to said terminals by the data broadcasting system.	12. System according to Claim 11, in which the secret code received by the master digital terminal and by the slave digital terminal is scrambled with the aid of keys sent beforehand to said terminals by the data broadcasting system.
13. A digital terminal intended to receive protected digital data, wherein the digital terminal can access said protected data only if information necessary for accessing said data and received by another digital terminal to which it can be connected, is sent to it by this other terminal within a predetermined deadline.	13. A digital terminal intended to receive protected digital data, wherein the digital terminal can access said protected data only if information necessary for accessing said data and received by another digital terminal to which it can be connected, is sent to it by this other terminal within a predetermined deadline.
14. A first digital terminal intended to be connected to a second digital terminal, wherein said first digital terminal is able to receive information necessary for said second terminal to access to protected digital data and is able to dispatch said information to said second terminal	14. A first digital terminal intended to be connected to a second digital terminal, wherein said first digital terminal is able to receive information necessary for said second terminal to access to protected digital data and is able to dispatch said information to said second terminal..

Conclusion

41. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. Yamamoto et al (Pub. No. US 2003/0084291 A1), was considered pertinent as showing transfer of encrypted data between two devices at the same premises. Also, *"5C Digital Transmission Content Protection White Paper"*, Rev. 1.0 on July 14, 1998 by Hitachi et al. was considered pertinent to the case for showing and explaining the use of DTCP, mentioned in one of the used references.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Omar Parra whose telephone number is 571-270-1449. The examiner can normally be reached on Under Academy Schedule.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Patrick Edouard can be reached on 571-272-7603. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

OP

PATRICK N. EDOUARD
SUPERVISORY PATENT EXAMINER